

Configuring 802.1X Authentication (CLI Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from denial-of-service (DoS) attacks and preventing unauthorized user access.

802.1X works by using an *Authenticator Port Access Entity* (the EX-series switch) to block all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking and opens the interface to the supplicant.

To configure 802.1X authentication:

- Specify the RADIUS server to be used as the authentication server.
 - Specify the 802.1X exclusion list, used to specify which supplicants can bypass 802.1X authentication and be automatically connected to the LAN.
 - Specify 802.1X interface settings on the switch.
1. Configuring the RADIUS Server on page 1
 2. Configuring Static MAC Bypass on page 2
 3. Configuring 802.1X Interface Settings on page 2

Configuring the RADIUS Server

To configure a RADIUS server:

1. Define the address of the server, the RADIUS server authentication port number, and the secret password. The secret password on the switch must match the secret password on the server:

```
[edit access ]
user@switch# set radius-server 10.0.0.100 port 1812 secret abc
```

2. Configure the authentication order, making radius the first method of authentication:

```
[edit access]
user@switch# set profile profile1 authentication-order radius
```

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:

```
[edit access profile]
user@switch# set profile1 radius authentication-server 10.0.0.100
10.2.14.200
```

Configuring Static MAC Bypass

Configure any MAC addresses, supplicants, or interfaces to be excluded from 802.1X authentication—that is, they will be authenticated.

To configure the 802.1X exclusion:

1. Specify a MAC address to be excluded from 802.1X authentication:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe
```

2. Configure a supplicant to bypass authentication if connected through a particular interface:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
```

3. Once a supplicant is authenticated, configure a supplicant to be moved to a specific VLAN:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
vlan-assignment default-vlan
```

Configuring 802.1X Interface Settings

Configure the supplicant mode, reauthentication, the administrative mode, and timeout values.

To configure the interface settings:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/5 supplicant multiple
```

2. Enable reauthentication:

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/5/0 reauthentication
interval 5
```

3. Configure the port timeout value for the response from the supplicant:

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/5 supplicant-timeout 5
```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

```
[edit protocols dot1x]  
user@switch# set authenticator interface ge-0/0/5 server-timeout 5
```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

```
[edit protocols dot1x]  
user@switch# set authenticator interface ge-0/0/5 transmit-period 60
```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols dot1x]  
user@switch# set authenticator interface ge-0/0/5 maximum-requests 5
```

- Related Topics**
- Configuring 802.1X Authentication (J-Web Procedure)
 - Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX-series Switch
 - Monitoring 802.1X Authentication
 - Verifying 802.1X Authentication
 - Configuring LLDP (CLI Procedure)
 - Understanding 802.1X Authentication on EX-series Switches

